

HN



## UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/822,548	03/30/2001	Matthew D. Wood	42390P10451	7654

7590 01/19/2005

Michael A. DeSanctis  
BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP  
Seventh Floor  
12400 Wilshire Boulevard  
Los Angeles, CA 90025-1026

EXAMINER

PYZOCHA, MICHAEL J

ART UNIT	PAPER NUMBER
----------	--------------

2137

DATE MAILED: 01/19/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

<b>Office Action Summary</b>	<b>Application No.</b> 09/822,548	<b>Applicant(s)</b> WOOD ET AL.	
	<b>Examiner</b> Michael Pyzocha	<b>Art Unit</b> 2137	

**-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --**

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 12 November 2004.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-9 and 17-24 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-9 and 17-24 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 30 March 2000 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All    b) ☐ Some \*    c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- |  |   |
|--|---|
| 1) <input checked="" type="checkbox"/> Notice of References Cited (PTO-892)  | 4) <input type="checkbox"/> Interview Summary (PTO-413)<br>Paper No(s)/Mail Date. _____ |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948)                                   | 5) <input type="checkbox"/> Notice of Informal Patent Application (PTO-152)             |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)<br>Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____  |

Art Unit: 2137

**DETAILED ACTION**

1. Claims 1-9 and 17-24 are pending and claims 10-16 are canceled.

***Election/Restrictions***

2. Claims 10-16 are withdrawn from further consideration pursuant to 37 CFR 1.142(b) as being drawn to a nonelected invention, there being no allowable generic or linking claim. Election was made **without** traverse in the reply filed on 11/12/2004.

***Claim Rejections - 35 USC § 103***

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

4. Claims 17-22, 24 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas Jr. et al (US 6687375) and further in view of Chen et al (US 6182220).

Art Unit: 2137

As per claim 17, Matyas Jr. et al discloses entropy enhancing system comprising: a local system comprising a pseudo-random number generator (PRNG) (see column 9 lines 19-34 and 45-67).

Matyas Jr. et al fails to disclose one or more remote independent systems comprising entropy servers.

However, Chen et al discloses one or more remote independent systems comprising entropy servers (see column 1 line 66 through column 2 line 9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to obtain the additional seeding information of Matyas Jr. et al from the server of Chen et al.

Motivation to do so would have been too update passwords on the server (see Chen et al column 4 lines 15-39).

As per claim 18, the modified Matyas Jr. et al and Chen et al system discloses the local system generates local seeding information (see Matyas Jr. et al column 9 lines 45-67).

As per claim 19, the modified Matyas Jr. et al and Chen et al system discloses the one or more remote independent systems generate remote seeding information (see Chen et al column 1 line 66 through column 2 line 9).

Art Unit: 2137

As per claim 20, the modified Matyas Jr. et al and Chen et al system discloses the entropy servers are machines (see Chen et al column 4 lines 40-54).

As per claim 21, the modified Matyas Jr. et al and Chen et al system discloses the entropy servers are software (see Chen et al column 5 lines 5-14).

As per claim 22, the modified Matyas Jr. et al and Chen et al system discloses the local system gathers the local seeding information (see Matyas Jr. et al column 9 lines 45-67).

As per claim 24, the modified Matyas Jr. et al and Chen et al system discloses the PRNG is stirred using the local seeding information and the remote seeding information (see Matyas Jr. et al column 9 lines 45-67).

5. Claims 1-3, 5-9, 23 are rejected under 35 U.S.C. 103(a) as being unpatentable over Matyas, Jr. et al, further in view of Chen et al and further in view of Hardy et al (US 6073242).

As per claim 1, Matyas Jr. et al discloses initializing a pseudo-random number generator (PRNG); obtaining local seeding information from a host; obtaining additional seeding information; and stirring the PRNG with the local seeding information and the additional seeding information (see column 9 lines 19-34 and 45-67).

Art Unit: 2137

Matyas Jr. et al fails to disclose securely obtaining additional seeding information from one or more remote and independent entropy servers.

However, Chen et al teaches obtaining seeding information from one or more remote and independent entropy servers (see column 1 line 66 through column 2 line 9).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to obtain the additional seeding information of Matyas Jr. et al from the server of Chen et al.

Motivation to do so would have been too update passwords on the server (see Chen et al column 4 lines 15-39).

The modified Matyas Jr. et al and Chen et al system fails to disclose the communication between host and server being secure.

However, Hardy et al teaches secure communications (see column 3 lines 54-67).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to muse Hardy et al's method of secure communications in the modified system of Matyas Jr. et al and Chen et al system.

Art Unit: 2137

Motivation to do so would have been to provide confidentiality, authentication and integrity to the communications (see column 3 lines 54-67).

As per claim 2-3, the modified Matyas Jr. et al, Chen et al and Hardy et al system discloses the initializing a PRNG comprises initializing the internal state of the PRNG with a random value that is a seed (see Matyas Jr. et al column 9 lines 19-34).

As per claim 5, the modified Matyas Jr. et al, Chen et al and Hardy et al system discloses the one or more remote and independent entropy servers maintain random state pool to supply the host with the random value (see Matyas Jr. et al column 9 lines 45-67).

As per claim 6-8, the modified Matyas Jr. et al, Chen et al and Hardy et al system discloses the securely obtaining seeding information from the one or more remote and independent entropy servers may include using a privacy protocol, wherein the privacy protocol comprises secure sockets layer (SSL) protocol and transport layer security (TLS) protocol (see Hardy et al column 3 lines 54-67).

As per claim 9, the modified Matyas Jr. et al, Chen et al and Hardy et al system discloses the stirring the PRNG comprises

Art Unit: 2137

producing a cryptographically random stream of bits (see Matyas Jr. et al column 9 lines 45-67).

As per claim 23, the modified Matyas Jr. et al, Chen et al and Hardy et al system discloses securely gathering the remote seeding information (see rejection as in claims 1 and 17).

6. Claim 4 is rejected under 35 U.S.C. 103(a) as being unpatentable over the modified Matyas Jr. et al, Chen et al and Hardy et al system as applied to claim 1 above, and further in view of AASAA et al (JP 08037138).

As per claim 4, the modified Matyas Jr. et al, Chen et al and Hardy et al system fails to disclose the securely obtaining seeding information from the one or more remote and independent entropy servers is repeated for redundant entropy servers.

However, AASAA et al teaches the method of repeating a process for redundant servers (see translated abstract).

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use AASAA et al's method of obtaining information from two servers in the modified Matyas Jr. et al, Chen et al, and Hardy et al system.

Motivation to do so would have been to compare the responses from both servers (see AASAA et al abstract).



**Conclusion**

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael Pyzocha whose telephone number is (571) 272-3875. The examiner can normally be reached on 7:00am - 4:30pm first Fridays of the bi-week off.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Caldwell can be reached on (571) 272-3868. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).



**ANDREW CALDWELL**  
**SUPERVISORY PATENT EXAMINER**